

Amendments to the Claims

1. (currently amended) A method of generating encrypted packets comprising the steps of:

~~generating at least one second~~ receiving in a security processor a first
Ethernet packet comprising ~~at least one first~~ a second Ethernet packet and ~~at least one a~~
memory address associated with ~~at least one~~ a security association;

~~extracting the at least one memory~~ address and the ~~at least one first~~ second
Ethernet packet from the ~~at least one second~~ first Ethernet packet;

~~retrieving at least one the~~ security association from ~~a at least one data~~
memory ~~according to the extracted at least one~~ using the received memory address; and

~~encrypting at least a portion of the extracted at least one first~~ second
Ethernet packet according to the retrieved ~~at least one~~ security association.

2. (currently amended) The method of claim 1 wherein the first Ethernet packet
also includes ~~generating step comprises generating an outer Ethernet header and another~~
a manufacturer header.

3. (currently amended) The method of claim 2 [[1]] wherein [[-]] the ~~another~~
manufacturer header comprises the at least one includes the memory address.

4. (currently amended) The method of claim 3 wherein the outer Ethernet header
comprises an Ethernet address of [[a]] the security processor.

5. (currently amended) The method of claim 4 wherein the outer Ethernet header comprises a ~~Broadcom-Ethernet~~ user-specific type field.

6. (currently amended) The method of claim 5 wherein a first byte of the manufacturer header is set to another header ~~comprises a zero~~.

7. (currently amended) The method of claim 6 wherein the second, third and fourth bytes of the manufacturer header ~~another header~~ ~~comprise the at least one~~ includes the memory address.

8. (canceled)

9. (currently amended) The method of claim 1 wherein the extracting step comprises determining whether an Ethernet type field from the ~~at least one second~~ first Ethernet packet comprises a ~~Broadcom~~ user-specific Ethernet type.

10-12. (canceled)

13. (currently amended) The method of claim 1 [[12]] wherein the retrieving step comprises retrieving the ~~at least one~~ security association from a ~~data~~ memory in [[a]] the security processor.

14. (currently amended) The method of claim 1 ~~[[13]]~~ wherein the encrypting step comprises using an encryption key associated with the ~~at least one~~ security association.

15. (currently amended) The method of claim 1 ~~[[13]]~~ wherein the encrypting step comprises using an encryption algorithm defined by the ~~at least one~~ security association.

16. (currently amended) The method of claim 1 wherein the extracting step comprises determining whether an Ethernet address from the ~~at least one second~~ first Ethernet packet matches an Ethernet address of ~~[[a]]~~ the security processor.

17. (currently amended) A method of generating encrypted packets by processing ~~at least one second~~ a first Ethernet packet comprising ~~at least one first~~ a second Ethernet packet and ~~at least one~~ a memory address associated with ~~at least one~~ a security association, the method comprising the steps of:

extracting the ~~at least one~~ memory address and the ~~at least one first~~ second Ethernet packet from the ~~at least one second~~ first Ethernet packet;

retrieving ~~at least one~~ the security association from ~~at least one data~~ a memory ~~according to the extracted at least one~~ using the extracted memory address; and

encrypting ~~at least a portion of the extracted at least one first~~ second Ethernet packet according to the retrieved ~~at least one~~ security association.

18. (currently amended) The method of claim 17 wherein the extracting step comprises determining whether an Ethernet type field from the ~~at least one second~~ first Ethernet packet comprises a ~~Broadcom~~ user-specific Ethernet type.

19. (currently amended) The method of claim 17 wherein the extracting step comprises determining whether a first byte following an Ethernet type field from the ~~at least one second~~ first Ethernet packet is set to a zero.

20. (currently amended) The method of claim 17 wherein the extracting step comprises extracting an address from second, third and fourth bytes following an Ethernet type field from the ~~at least one second~~ first Ethernet packet.

21. (currently amended) The method of claim 17 wherein the extracting step comprises extracting an address from a ~~the~~ lower 22 bits of second, third and fourth bytes following an Ethernet type field from the ~~at least one second~~ first Ethernet packet.

22. (currently amended) The method of claim 17 wherein the retrieving step comprises retrieving the ~~at least one~~ security association from a ~~data~~ memory in a security processor.

23. (currently amended) The method of claim 17 wherein the encrypting step comprises using an encryption key associated with the ~~at least one~~ security association.

24. (currently amended) The method of claim 17 wherein the encrypting step comprises using an encryption algorithm defined by the ~~at least one~~ security association.

25. (currently amended) The method of claim 17 wherein the extracting step comprises determining whether an Ethernet address from the ~~at least one second~~ first Ethernet packet matches an Ethernet address of a security processor.

26. (currently amended) A method of generating packets to be encrypted comprising the steps of:

generating ~~at least one~~ a first Ethernet packet;

associating ~~at least one~~ a security association with the ~~at least one~~ first Ethernet packet;

identifying ~~at least one~~ a memory address associated with the ~~at least one~~ security association; and

generating ~~at least one~~ a second Ethernet packet encapsulating the memory comprising the ~~at least one~~ address and the ~~at least one~~ first Ethernet packet.

27. (currently amended) The method of claim 26 wherein the generating step a second Ethernet packet comprises generating an outer Ethernet header comprising an address of a security processor.

28. (currently amended) The method of claim 26 wherein the generating a second Ethernet packet step comprises generating an outer Ethernet header and ~~another~~ a

manufacturer header.

29. (original) The method of claim 28 wherein the outer Ethernet header comprises an Ethernet address of a security processor.

30. (currently amended) The method of claim 28 wherein the outer Ethernet header comprises a ~~Broadcom~~ user-specified Ethernet type field.

31. (currently amended) The method of claim 28 wherein the ~~another~~ manufacturer header comprises the ~~at least one~~ memory address.

32. (currently amended) The method of claim 28 wherein a first byte of the manufacturer header is set to another header ~~comprises a~~ zero.

33. (currently amended) The method of claim 28 wherein second, third and fourth bytes of the ~~another~~ manufacturer header comprise the ~~at least one~~ memory address.

34. (canceled)

35. (currently amended) The method of claim 26 further comprising the steps of:
receiving data to be sent over an Ethernet network; and
incorporating the data into the ~~at least one~~ first Ethernet packet.

36. (currently amended) The method of claim 26 further comprising the step of transmitting the ~~at least one~~ second Ethernet packet to at least one security processor.

37. (currently amended) A security processor for generating encrypted packets by processing ~~at least one second~~ a first Ethernet packet comprising ~~at least one first~~ a second Ethernet packet and ~~at least one~~ a memory address associated with ~~at least one~~ a security association, comprising:

~~at least one data~~ a memory for storing ~~at least one the~~ security association;

~~at least one~~ a Gigabit MAC for receiving ~~at least one second~~ the first Ethernet packet;

~~at least one~~ a processor, connected to receive at least a portion of the ~~at least one second~~ first Ethernet packet from the ~~at least one~~ Gigabit MAC, for

extracting ~~at least one the~~ memory address from the ~~at least one second~~ first Ethernet packet; and

retrieving ~~at least one the~~ security association from the ~~at least one data~~ memory ~~according to~~ using the extracted ~~at least one~~ memory address; and

~~at least one an~~ encryption processor, connected to the ~~at least one~~ processor, for encrypting at least a portion of the ~~at least one first~~ second Ethernet packet according to the retrieved ~~at least one~~ security association.

38. (currently amended) The security processor of claim 37 wherein the ~~at least one second~~ first Ethernet packet comprises an outer Ethernet header and ~~another~~ a manufacturer header ~~and the another header comprises the at least one~~ including the

memory address.

39. (currently amended) The security processor of claim 37 wherein the ~~at least one~~ encryption processor comprises an ~~at least one~~ IPsec processor.

40. (original) The security processor of claim 37 wherein the security processor is an integrated circuit.

41-53. (canceled)